CLAIMS

What is claimed is:

Sub a2

1. In a firewall device having a plurality of communication interfaces, a packet filtering component coupled to each of the interfaces, a switching component coupled to each of the interfaces, and a firewall services component coupled to the switching process, a firewall system comprising:

a) a session manager operating in said firewall services component, said session manager structured and configured to instantiate a plurality of sessions in said firewall services component and a plurality of mini-sessions in said switching process component, each said session having header and payload information related to a corresponding data transfer within the firewall device, each said mini-session corresponding to a session and including header information related the corresponding data transfer within the firewall device; and

b) a firewall module operating in said switching process coupled to said mini-sessions, said firewall module configured to intercept data packets received into the interfaces, said firewall module further configured to track session context of said data packets.

2. The firewall system of claim 1, wherein said session manager is further structured and configured to manage said sessions and said mini-sessions.

3. The firewall system of claim 1, wherein said session manager is further structured and configured to delete said sessions and said mini-sessions.

4. The firewall system of claim 1, wherein said firewall module is further configured to intercept data packets before reception by said packet filtering component, said firewall module further configured to set a "pass" flag in data packets according matching header information in intercepted data packets and said header information in said mini-sessions.

5. The firewall system of claim 4, wherein said packet filtering component is configured to bypass "Access Control List" authorization of data packets having a "pass" flag.

6. The firewall system of claim 1, wherein said firewall module is further configured to intercept data packets before reception by said packet filtering component, said firewall module further configured to set a "do not divert" flag in data packets when packet inspection of said intercepted data packets does not require application-level inspection.

7. The firewall system of claim 6, wherein said firewall module is configured to bypass authorization of data packets having a "do not divert" flag with said firewall services component.

8. In a firewall device having a plurality of communication interfaces, a packet filtering component coupled to each of the interfaces, a switching component

coupled to each of the interfaces, and a firewall services component coupled to the switching process, a method for optimizing firewall processing comprising:

a) providing a session manager in the firewall services component;

b) providing a firewall module in the switching component;

c) instantiating a session, by said session manager, for data transfers within the firewall device, said sessions having header and payload information related to data transfers within the firewall device; and

d) instantiating a mini-session, by said session manager, corresponding to said instantiated session, said mini-session having header information related to data transfers within the firewall device.

9. The method of claim 8, further comprising:

a) intercepting data packets having a header and a payload component, by said firewall module, before reception by the packet filtering component; and

b) setting a "pass" flag in the intercepted data packets when said header component is the intercepted data packets matches said header information in said mini-session.

10. The method of claim 8, further comprising:

a) checking data packets for a "pass" flag, by said packet filtering component; and

b) bypassing "access control list" check, if a "pass" flag is found in said checked data packets.

11. The method of claim 8, further comprising:

a) intercepting data packets having a header and a payload component, by said firewall module, before reception by the packet filtering component; and

b) setting a "do not divert" flag in the intercepted data packets when packet inspection does not require application-level inspection.

12. The method of claim 8, further comprising:

a) checking data packets for a "do not divert" flag, by said firewall module; and

b) bypassing "access control list" check, if a "do not divert" flag is found in said checked data packets.

13. The method of claim 8, further comprising bypassing authorization with the firewall services component, by the firewall module, for data packets header information matching header information in said mini-sessions.

14. The method of claim 8, further comprising deleting said session and associated mini-session when data transfer associated with said sessions and mini-session is completed.

15. The method of claim 8, further comprising deleting said session and associated mini-session when data transfer associated with said sessions and mini-session is idle past a predetermined timeout period.

16. The method of claim 8, further comprising updating context of said mini-session, by said firewall module, without sending packets to said firewall services component.

17. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for optimizing firewall processing in a firewall device having a plurality of communication interfaces, a packet filtering component coupled to each of the interfaces, a switching component coupled to each of the interfaces, and a firewall services component coupled to the switching process, said method comprising:

a) providing a session manager in the firewall services component;

b) providing a firewall module in the switching component;

c) instantiating a session, by said session manager, for data transfers within the firewall device, said sessions having header and payload information related to data transfers within the firewall device; and

d) instantiating a mini-session, by said session manager, corresponding to said instantiated session, said mini-session having header information related to data transfers within the firewall device.

18. The program storage device of claim 17, said method further comprising:

a) intercepting data packets having a header and a payload component, by said firewall module, before reception by the packet filtering component; and

b) setting a "pass" flag in the intercepted data packets when said header component is the intercepted data packets matches said header information in said mini-session.

19. The program storage device of claim 17, said method further comprising:

a) checking data packets for a "pass" flag, by said packet filtering component; and

b) bypassing "access control list" check, if a "pass" flag is found in said checked data packets.

20. The program storage device of claim 17, said method further comprising:

a) intercepting data packets having a header and a payload component, by said firewall module, before reception by the packet filtering component; and

b) setting a "do not divert" flag in the intercepted data packets when said intercepted data packets packet inspection does not require application-level inspection.

21. The program storage device of claim 17, said method further comprising:

a) checking data packets for a "do not divert" flag, by said firewall module; and

b) bypassing "access control list" check, if a "do not divert" flag is found in said checked data packets.

22. The program storage device of claim 17, said method further comprising bypassing authorization with the firewall services component, by the firewall module, for data packets header information matching header information in said mini-sessions.

23. The program storage device of claim 17, said method further comprising deleting said session and associated mini-session when data transfer associated with said sessions and mini-session is completed.

24. The program storage device of claim 17, said method further comprising said session and associated mini-session when data transfer associated with said sessions and mini-session is idle past a predetermined timeout period.

25. The program storage device of claim 17, said method further comprising updating context of said mini-session, by said firewall module, without sending packets to said firewall services component.